

CPNI Regulations

The following CPNI rules will apply to E Street:

(1) Training. Personnel must be trained as to when they are and are not authorized to use CPNI, and E Street must have an express disciplinary process in place for violations of the CPNI policies.

(2) Certification. An officer, as an agent of E Street, must sign and file with the FCC a compliance certificate on an annual basis. In the certification, the officer must state that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the CPNI rules. E Street must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the CPNI rules. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

(3) Use of CPNI without customer approval.

(i) E Street may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service to which the customer already subscribes from E Street without customer approval. If E Street provides different categories of service, and a customer subscribes to more than one category of service, E Street may share CPNI among affiliated entities that provide a service offering to the customer. E Street is not otherwise permitted to share CPNI with any affiliates. E Street may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from E Street, unless it has customer approval to do so.

(ii) E Street may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

(iii) E Street may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(iv) E Street may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, allow billing by its resale customers, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

(v) E Street must maintain a record, electronically or in some other manner, of its own and its affiliates' sales and marketing campaigns that use its customers' CPNI. E Street must maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. E Street must retain the record for a minimum of one year.

(vi) E Street must establish a supervisory review process regarding carrier compliance with the rules for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

(4) Approval required for use of CPNI. E Street may obtain approval through written, oral or electronic methods. If E Street chooses to use oral approval, it must be prepared to prove to the FCC that approval has been given. Records of approval must be maintained for at least one year. Generally, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

(i) **General Notice Requirements.** Prior to any solicitation for customer approval, E Street must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit E Street to use, disclose, or permit access to, the customer's CPNI. The notification must state that the customer has a right, and E Street has a duty, under federal law, to protect the confidentiality of CPNI. The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time. The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, E Street may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI. The notification must be comprehensible and must not be misleading. If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer. If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language. E Street may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. E Street also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer. E Street may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI. The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial. Solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(ii) **Notice Requirements Specific to Opt-Out.** E Street must provide notification to obtain opt-out approval through electronic or written methods, but generally not by oral communications. E Street must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. E Street must notify customers as to the applicable waiting period for a response before approval is assumed. In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and in the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed. Carriers using the opt-out mechanism must provide notices to their customers every two years.

Carriers must provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly. The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information. Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

(a) **E-mail Opt-Out Requirements.** Carriers that use e-mail to provide opt-out notices must comply with additional requirements. Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in

particular. Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out. Opt-out e-mail notices that are returned as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice. Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail. Carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(iii) Notice Requirements Specific to One-Time Use of CPNI. Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact. Carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election. Carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party. Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use. Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

(5) Safeguards for use of CPNI. E Street must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including properly authenticating a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(i) Telephone access to CPNI. E Street may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, E Street may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to E Street during a customer-initiated call without E Street's assistance, then E Street is permitted to discuss the call detail information. To establish a password, E Street must authenticate the customer without the use of readily available biographical information, or account information. E Street may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password.

(ii) Online access to CPNI. E Street must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password that is not prompted by the carrier asking for readily available biographical information, or account information.

(6) Notification of account changes. E Street must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the

telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(7) Business customer exemption. Telecommunications carriers may bind themselves contractually to authentication regimes other than those described above for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

(8) Notification of customer proprietary network information security breaches.

(a) E Street must notify law enforcement of a breach of its customers' CPNI as provided in this section. E Street must not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement.

(b) As soon as practicable, and no later than seven (7) business days, after reasonable determination of the breach, E Street must electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The FCC will maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>.

(c) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below. After E Street has completed the process of notifying law enforcement it shall notify its customers of a breach of those customers' CPNI. If E Street believes that there is an extraordinarily urgent need to notify any class of affected customers sooner, it may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. E Street must cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(9) Recordkeeping. E Street must maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. E Street must retain the record for a minimum of 2 years.